

A Toyota és a Mazda együtt próbálják kivédeni az autóikat érő kibertámadásokat

Új korszak, új problémák. Mivel az autók világa is egyre inkább szerves része a kibertérnek, a felelősen viselkedő gyártóknak új problémákkal is szembe kell nézniük.

Kétségtelen tény, hogy a konnektivitás az autókban óriási előrelépésnek számít. Egyrészt megkönnyíti a diagnosztikát és lehetővé teszi a felhőalapú szoftverfrissítéseket, másrészt nagyon sok olyan funkció válik elérhetővé a felhasználók számára, amelyek egyszerűbbé és élvezetesebbé teszik az autó birtoklását.

Egy-egy autóban ma már ezer mikrochip van, s a kocsi különböző egységei kapcsolódnak az internetre és kommunikálnak más eszközökkel, online szerverekkel. Így olyan előnyöket élvezhetünk, mint a valós idejű forgalmi információk, amelyek segítenek kikerülni egy-egy torlódást és így időt, üzemanyagot takarítanak meg. Vagy ott vannak az online szoftverfrissítések, amelyekkel a felhasználónak csupán annyi a dolga, hogy jóváhagyja a fedélzeti rendszer képernyőjén. Szintén fontos képessége az internetre kapcsolt rendszereknek, hogy baleset nyomán automatikusan segítséget hívnak. Nem csoda, hogy az ilyen rendszerrel felszerelt autók száma gyors mértékben nő. Míg 2021-ben 237 millió autó bírt internetkapcsolattal, addig jövőre ez a szám 400 millió fölé nő.

Mindennek azonban ára van. Ami ugyanis kapcsolódik az internetre, ahhoz rossz szándékkal is hozzá lehet férni. A legjobb esetben ez csak annyit tesz, hogy adatlopás történik, legrosszabb esetben – ahogy ez már meg is történt az Egyesült Államokban – a hacker fizikai értelemben is átveszi az irányítást az autó fölött és balesetet okozhat.

A gyártóknak erre az új fenyegetésre választ kell találniuk. Ezért fogott össze a Toyota, a Mazda és a Hitachi, az Aisin és a Denso, hogy olyan kiberbiztonsági tervet dolgozzanak ki, amely vonatkozik a beszállítókra, a teljes beszállítási láncra, valamint a szervizpontokra is, de már a fejlesztés és a gyártás során is alkalmazzák majd az új alapelveket. Az új kiberbiztonsági sztenderdek vonatkoznak majd a biztonságosabb szoftverekre, illetve a védett komponensek olyan közös készletére, amelyeket a márkák közösen használnak.

Magyarul az a terv, hogy egyszer csinálják meg jól, aztán használják közösen, hiszen ha minden beszállító és gyártó betartja a közösen hozott szabályokat, akkor a kocsiban futó programok sem válnak sebezhetővé. Így ugyanis nemcsak az online frissítések válhatnak olyan gyakorivá, amennyire szükséges, de a felhasználók élete is egyszerűbb lesz.

Manapság még messze nem tartunk itt, hiszen ugyanannak a funkciónak még a neve is eltér a különböző márkák autóiban; intelligens sebességtartó automatika, adaptív sebességtartó automatika, okos sebességtartó automatika. Bár a Toyota autóit nem érte kibertámadás, a japán márkák a fejlesztési és programozási szabályok egységesítésben, valamint a közösen használt, biztonságos komponensek alkalmazásában látja a jövőt.

Fotók: *Top Gear, Automotive News, IT Security Guru*

Forrás:

<https://news.smartermedia.hu/nemzetkozi-hirek/a-toyota-es-a-mazda-egyutt-probaljak-kive-deni-az-autoikat-ero-kibertamadasokat>